



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 19, 2021

VIA E-MAIL ONLY

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
E-mail: ndag@nd.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Tax Sheltered Compensation, Inc. ("TSC") located at 7300 Metro Boulevard, #450, Edina, Minnesota 55439, and are writing to supplement our June 14, 2021 notice to your office of a security incident attached here as ***Exhibit AA***. By providing this notice, TSC does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 15, 2021 TSC was informed that Netgain, a cloud hosting company that was used to house data related to TSC's clients, experienced a ransomware incident. Communications from Netgain stated that Netgain's environment was subject to unauthorized access beginning in late September 2020. Per Netgain's investigation, there was evidence that certain data was exfiltrated from their environment between September 2020 and December 3, 2020.

TSC conducted an extensive review of the entire contents of the impacted files as provided by Netgain. On March 31, 2021, TSC's investigation confirmed that the individuals to whom the impacted data related. As the impacted data was related to individuals associated with TSC's clients, TSC then notified the impacted clients and provided information about the incident and the impacted individuals.

From May 19, 2021 to May 26, 2021 TSC received authorization and address information from certain TSC clients. TSC provided notice to impacted individuals and regulators, as required, on behalf of its clients.

The information that could have been subject to unauthorized access includes name, date of birth, and Social Security Number for two hundred ninety seven (297) North Dakota residents.

Following that, TSC received authorization and address information from additional clients. TSC is now providing supplemental notice to account for that additional population.

Notice to North Dakota Residents

On or about July 19, 2021, TSC provided written notice of this incident to all affected individuals, which includes one thousand one hundred eighty five (1,185) North Dakota residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, TSC moved quickly to investigate and respond to the incident, assess the security of TSC systems, and notify potentially affected individuals. TSC is also working to implement additional safeguards and training to its employees. TSC is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TSC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. TSC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/meg
Enclosure

EXHIBIT AA

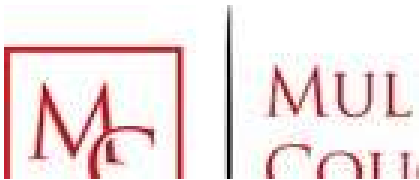
From: Meagan Gordon
Sent: Monday, June 14, 2021 5:23 PM
To: ndag@nd.gov
Cc: Vince Regan; Susan Fuster-Marin; April Cox-Lockridge
Subject: Tax Sheltered Compensation, Inc. - Notice of Data Event -
Attachments: TSC - ND - Notice of Data Event.pdf

Dear Sir or Madam,

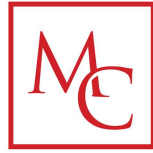
Please see the attached Notice of Data Event.

Thank you,
Meagan Gordon

Meagan Gordon
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-4863 - Office
(925) 519-1349 - Mobile
mgordon@mullen.law



This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 14, 2021

VIA E-MAIL

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
E-mail: ndag@nd.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Tax Sheltered Compensation, Inc. ("TSC") located at 7300 Metro Boulevard, #450, Edina, Minnesota 55439, and are writing to notify your office of an incident that may affect the security of some personal information relating to two hundred ninety seven (297) North Dakota residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TSC does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 15, 2021 TSC was informed that Netgain, a cloud hosting company that was used to house data related to TSC's clients, experienced a ransomware incident. Communications from Netgain stated that Netgain's environment was subject to unauthorized access beginning in late September 2020. Per Netgain's investigation, there was evidence that certain data was exfiltrated from their environment between September 2020 and December 3, 2020.

TSC conducted an extensive review of the entire contents of the impacted files as provided by Netgain. On March 31, 2021, TSC's investigation confirmed that the individuals to whom the impacted data related. As the impacted data was related to individuals associated with TSC's clients, TSC then notified the impacted clients and provided information about the incident and the impacted individuals.

From May 19, 2021 to May, 26, 2021 TSC received authorization and address information from certain TSC clients. TSC is providing notice to impacted individuals and regulators, as required, on behalf of its clients.

The information that could have been subject to unauthorized access includes name, address, Social Security number, and date of birth.

Notice to North Dakota Residents

On or about June 14, 2021, TSC provided written notice of this incident to all affected individuals, which includes two hundred ninety seven (297) North Dakota residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, TSC moved quickly to investigate and respond to the incident, assess the security of TSC systems, and notify potentially affected individuals. TSC is also working to implement additional safeguards and training to its employees. TSC is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TSC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. TSC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/meg

Exhibit A

Tax Sheltered Compensation, Inc.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Tax Sheltered Compensation, Inc. (“TSC”) is a third-party retirement plan administration firm that recently acquired certain business from Corporate Benefit Administrators, Inc. (“CBA”). TSC and / or CBA, Inc. have provided retirement plan administration services to <<b2b_text_1(Client)>>. This letter is intended to notify you of an incident that may affect the privacy of some of your information. We take the protection of your information very seriously, and this letter provides details regarding the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On January 15, 2021 TSC was informed that Netgain, a cloud hosting company that was used to house data related to <<b2b_text_1(Client)>>, experienced a ransomware incident. Communications from Netgain stated that Netgain’s environment was subject to unauthorized access beginning in late September 2020. Per Netgain’s investigation, there was evidence that certain data, including data relating to individuals associated with <<b2b_text_1(Client)>>, was exfiltrated from their environment between September 2020 and December 3, 2020.

TSC conducted an extensive review of the entire contents of the impacted files as provided by Netgain. On March 31, 2021, TSC’s investigation confirmed that the impacted data included certain information relating to you.

What Information Was Involved? The personal identifiable information relating to you includes your name, date of birth, and Social Security number.

What Are We Doing? The privacy and security of information are among one of our highest priorities, and TSC has strict security measures in place to protect information in our care.

In an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also providing identity monitoring services for 12 months through Kroll at no cost to you. Information and instructions on how to activate these complimentary services can be found in the “Steps You Can Take to Help Protect Your Information” attached to this letter.

What Can You Do? While TSC has not received reports of any actual or attempted misuse of your information related to this incident, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You may review the information contained in the attached “Steps You Can Take to Help Protect Your Information.” You may also activate to receive the identity monitoring services we are making available to you. There is no charge to you for the cost of this service; however, you will need to activate yourself in this service.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-731-2987 (toll free), Monday through Friday, 8:00 a.m. to 5:30 p.m., Central Time excluding major US holidays.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Tax Sheltered Compensation, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **October 18, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;

4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160 Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Tax Sheltered Compensation, Inc. is located at 7300 Metro Boulevard, Suite #450, Edina, MN 55439.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.